VA-NSOC

DEPARTMENT OF VETERANS AFFAIRS
Information Technology Field Operations
Field Security Operations
Network and Security Operations Center (NSOC)

Monthly Report to Congress of Data Breaches

May 03 - 30, 2010

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0328230	Privacy	VBA Waco, TX	5/3/10	5/7/10	18	Moderate	1
Date US-CERT Notified	**US-CERT Case Number**	**Date Privacy Notified**	**(Old)PVTS Number**	**Date OIG Notified**	**Accepted by OIG**	**OIG Case Number**	**No. of Loss Notifications**
5/3/2010	INC000000090147	N/A		N/A		N/A	0

Incident Summary

Veteran A received a letter from WACO RO with Veteran B's letter in the envelope. The letter contained Veteran B's name and full social security number.

Incident Update

05/04/10:
Veteran B will receive a letter offering credit protection services.

NOTE: There were a total of 123 Mis-Mailed incidents this reporting period. Because of repetition the other 122 are not included in this report, but are included in the "Mis-Mailed Incidents" count at the end of this report. In all incidents Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

Resolution

The employee received counseling. The credit monitoring letter was sent.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0329101	Privacy	VISN 17 Dallas, TX	5/4/10	5/25/10	5	High	4,083
Date US-CERT Notified	**US-CERT Case Number**	**Date Privacy Notified**	**(Old)PVTS Number**	**Date OIG Notified**	**Accepted by OIG**	**OIG Case Number**	**No. of Loss Notifications**
5/4/2010	INC000000090410	N/A		N/A		N/A	0

Incident Summary

A binder and clip board containing approximately 3,265 Veteran's names, social security numbers, dates of birth and lab tests to be drawn is missing from a secured access laboratory area. The time frame that the binder covered was February, March and April 2010.

Incident Update

05/11/10:
The 3265 Veterans will receive a letter offering credit protection services. This issue will be reported to HHS under the new HITECH Act.

05/17/10:
An additional 818 Veterans' PII was in the information missing.

05/25/10:
The information was entered into the HHS web portal. RMIR was contacted by HHS/OCR representative to verify information.

Resolution

The credit monitoring letters were sent. Pathology and Laboratory Medicine Service are no longer using log sheets or binders to track patient workload.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0331775	Privacy	VISN 07 Birmingham, AL	5/10/10	6/1/10	38	Moderate	0
Date US-CERT Notified	**US-CERT Case Number**	**Date Privacy Notified**	**(Old)PVTS Number**	**Date OIG Notified**	**Accepted by OIG**	**OIG Case Number**	**No. of Loss Notifications**
5/10/2010	INC000000091239	N/A		N/A		N/A	101

Incident Summary

An inpatient and Emergency Room patient listing was taken from the AOD's office by a non-employee/unauthorized individual. The Inpatient Listing consisted of 101 names, last 4 of social security numbers, ward/room number, religious preference and inpatient condition. The Emergency Unit listing consisted of 4 names and check-in times into the ER only.

Incident Update

05/11/10:
One hundred and one (101) Patients will receive notification letters.

NOTE: There were a total of 74 Mis-Handling incidents this reporting period. Because of repetition the other 73 are not included in this report, but are included in the "Mis-Handling Incidents" count at the end of this report. In all incidents Veterans will receive a notification letter and/or credit monitoring will be offered if appropriate.

Resolution

The notification letters have been sent. Procedures have been implemented to ensure this type of incident does not occur again, including instructing staff to lock office doors when they leave the office.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0333721	Privacy	VISN 12 North Chicago, IL	5/13/10		52	High	10
Date US-CERT Notified	**US-CERT Case Number**	**Date Privacy Notified**	**(Old)PVTS Number**	**Date OIG Notified**	**Accepted by OIG**	**OIG Case Number**	**No. of Loss Notifications**
5/13/2010	INC000000091817	N/A		5/14/2010		Pending	0

Incident Summary

A VA clinical supervisory employee reported that the records of 10 employees (including his own employee record) were missing from the office. Apparently someone having a key entered the office overnight, broke into the locked desk and took the records. Eight of those employees are also Veterans. The VA police are investigating.

Incident Update

05/17/10:
The office was locked but several of the clinical staff had keys to this office. The missing records contained full name, full SSN, DOB, address, phone number, emergency contacts with their address and phone number, DD214 (paper Veterans receive upon discharge which may or may not contain medical information), resume, and education transcripts. Eight (8) Veterans and two (2) employees will be offered credit protection services.

06/04/10:
The VA police concluded their investigation. The records were not located.

Resolution

The PO instructed the employee to retake the Privacy training. The lock on the door to the office has been rekeyed and the supervisor has the only key.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0333733	Missing/Stolen VA Resources	VISN 08 Bay Pines, FL	5/13/10	5/23/10	22	Low	
Date US-CERT Notified	**US-CERT Case Number**	**Date Privacy Notified**	**(Old)PVTS Number**	**Date OIG Notified**	**Accepted by OIG**	**OIG Case Number**	**No. of Loss Notifications**
5/13/2010	INC000000091819	N/A		N/A		N/A	

Incident Summary

On 05/13/10 at approximately 10:40 AM, the ISO was notified of an incident involving 2 missing/stolen patient laptops which were either purchased by or donated to the Recreation Therapy Service (RTS) for patient use (email, games, etc). These laptops had no connectivity to the VA network, nor were they used for direct patient care. These laptops were not encrypted and no PII/PHI was stored on the devices.

Incident Update

05/14/10:
The RTS laptops were secured in the a storage room. Computers are distributed by the RTS clinic staff to the patients. In the patient rooms the computer lock/cable system is used to secure the computer. The RTS staff did not keep a written log but the computers were seen in the storage room the week of 05/03/10. The staff noticed them missing on 05/10/10 when staff went to get them so they could be taken for servicing and virus updates installed.

The RTS computer program started before encryption was required by the VA. They are not network computers they do not have any VA data on them. They are in no way connected to the VA Intranet or CPRS. They are for patient recreational use only.

Resolution

These laptops were not purchased by OI&T. The laptops were purchased by TRS with General Post Fund Money donated by a service organization for the purchase of the computers for patient treatment and recreational use. The two computers were purchased by the American Legion 273 and then donated to TRS.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0333820	IT Equipment Inventory	EMPLOYEE EDUCATION SERVICE/ EES St. Louis, MO	5/13/10	5/18/10	15	Low	
Date US-CERT Notified	**US-CERT Case Number**	**Date Privacy Notified**	**(Old)PVTS Number**	**Date OIG Notified**	**Accepted by OIG**	**OIG Case Number**	**No. of Loss Notifications**
5/13/2010	INC000000091861	N/A		N/A		N/A	

Incident Summary

As part of an IT Equipment Inventory, an external hard drive was not located. The drive was unencrypted. It was purchased over 5 years ago when the encryption requirement was not in place. The drive stored multimedia files for e-learning initiatives and did not contain sensitive or PII/PHI data. The Inventory team agreed this drive was inadvertently picked up as part of mass equipment turn-in to host Cleveland VAMC in October 2009, and not recorded on turn-in paperwork. The Report of Survey is being prepared and local VA police will be contacted for Police Report number.

Incident Update

05/17/10:
Within the EIL database it states, "the drive was visually verified on 08/13/09 with note that the drive was turned in 08/17/09."
The supporting turn-in paperwork cannot be located.

NOTE: There were a total of 4 IT Equipment Inventory Incidents this reporting period. Because of repetition the other 3 are not included in this report, but are included in the "IT Equipment Inventory Incidents" count at the end of this report.

Resolution

The Police Report and Report of Survey have been completed. The Police Report states "no further action needed at this time."

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0334872	Privacy	VHA CMOPMURFREESBORO, TN	5/16/10		45	Moderate	0
Date US-CERT Notified	**US-CERT Case Number**	**Date Privacy Notified**	**(Old)PVTS Number**	**Date OIG Notified**	**Accepted by OIG**	**OIG Case Number**	**No. of Loss Notifications**
5/16/2010	INC000000092201	N/A		N/A		N/A	6

Incident Summary

The Murfreesboro Consolidated Mail Outpatient Pharmacy (CMOP) was notified by the UPS Investigator, that bottles of medication for six (6) VA patients were found in a UPS employee's possession. The packaging and prescription documents were missing. The patient's name, address and medication have been compromised. The UPS employee has been arrested for multiple thefts of VA prescription packages. The VA OIG has been notified. The medical centers have been notified to contact provider for replacement.

Incident Update

05/17/10:
The six Veterans will receive letters of notification.

NOTE: There were a total of 22 Mis-Mailed CMOP incidents out of 5,793,986 total packages (8,705,272 total prescriptions) mailed out for this reporting period. Because of repetition the other 21 are not included in this report, but are included in the "Mis-Mailed CMOP Incidents" count at the end of this report. In all incidents Veterans will receive a notification letter.

VA-NSOC Incident Number	Incident Type	Organization	Date Opened	Date Closed	FERET Score	Risk Category	No. Of Credit Monitoring
VANSOC0335815	Privacy	VISN 20 Walla Walla, WA	5/18/10	5/27/10	38	Moderate	50
Date US-CERT Notified	**US-CERT Case Number**	**Date Privacy Notified**	**(Old)PVTS Number**	**Date OIG Notified**	**Accepted by OIG**	**OIG Case Number**	**No. of Loss Notifications**
5/18/2010	INC000000092559	5/18/2010		N/A		N/A	36

Incident Summary

Documents containing information on 250 Veterans were found in the chemical dependency day room. These included a listing of outside nursing home facilities' Veteran residents' names and last 4 of their social security numbers. A second listing of Veterans in the chemical dependency program, including their names, ages, dates of birth, last 4 of their social security numbers and medical information including PHI was also found.

Incident Update

05/27/10:
According to the PO, the total count was not 250 but 86 Veterans. There were 36 Veterans whose PHI and 50 Veterans whose PII was exposed. Therefore 36 Veterans will receive a notification letter and 50 Veterans will receive a letter offering credit protection services.

Resolution

The notification and credit monitoring letters were sent.

Total number of lost Blackberry incidents	13
Total number of internal un-encrypted e-mail incidents	80
Total number of Mis-Handling Incidents	74
Total number of Mis-Mailed Incidents	123
Total number of Mis-Mailed CMOP Incidents	22
Total number of IT Equipment Inventory Incidents	4
Total number of Missing/Stolen PC Incidents	0
Total number of Missing/Stolen Laptop Incidents	6 (5 encrypted)